Exposé :

Cyberrésilience : Enjeux et Défis

Présenté par Djiby Sow, Professeur à UCAD-Dakar-Sénégal
sowdjibab@yahoo.fr, djiby.sow@ucad.edu.sn

Technlogies émergentes et cyberrésilience

Technlogies émergentes et cyberrésilience

Il y a 60 ans, à l'aube des indépendences, l'Afrique a raté le virage du nucléaire civil avec des avatages considérables pour la santé, l'énergie/l'électricté, le déssalement de l'eau, l'agriculture, la fabrication d'hydrogène etc.

Il faut pas que l'Afrique fasse les mêmes erreurs avec les technologies émergentes : Cyberdéfense, Cryptographie post quantique, Intelligence Artificielle, Blockchain, Cloud, Quantum computing, IoT, Edge computing, Réalité augmentée etc..

Technlogies émergentes et cyberrésilience

Technlogies émergentes et cyberrésilience

Le developpement fulgurant de la cybercriminalité ces dernières années est un frein à la souveraineté et au développement des pays africains (problèmes de compétitivité des entreprises, de protection des infrastructures et systèmes critiques, de vol de données stratégiques, d'espionnage, de désinformation de masse sur les réseaux sociaux, de guerre des drones, de cyber-renseignement étranger etc.)

Technlogies émergentes et cyberrésilience

Quelques chiffres et motivations pour la cyberrésilience

SMSI 2023 fixe le cap : créer une société numérique prospère, résiliente aux cybermenaces et dotée des connaissances et des capacités nécessaires pour exploiter les opportunités et gérer les risques

Mais la situation n'est pas rose pour l'Afrique.

Technlogies émergentes et cyberrésilience

Quelques chiffres et motivations pour la cyberrésilience

Mais la situation n'est pas rose pour l'Afrique.

- D'après le **rapport ECA 2022, la cybersécurité africaine est immature** par rapport à d'autres régions, ce qui rend le continent vulnérable aux cyberattaques, car **le marché numérique africain devrait atteindre 712 milliards de dollars d'ici 2050**.
- D'après le **Rapport Sommet Mondial de Société de l'Information SMSI 2023/Afrique**, le faible niveau de préparation de l'Afrique en matière de cybersécurité **coûte aux États membres en moyenne 10 % de leur PIB**

Technlogies émergentes et cyberrésilience

Quelques chiffres et motivations pour la cyberrésilience

Forum économique mondial (Global Risks Report 2022) : la cyberrésilience dans le top 10 des risques les plus sévères du monde et non dans le top 5 :

Technological risks—such as "digital inequality" and "cybersecurity failure"—are other critical short- and medium-term threats to the world according to GRPS respondents, but these fall back in the rankings towards the long term and none appear among the most potentially severe, signalling a possible blind spot in risk perceptions.

Les principales raisons sont **(1) le cyberespace est un écosystème dans lequel les acteurs mettent en place régulièrement des solutions de cyberésilience depuis 40 ans (2) les coûts sont moindres, (3) l'accord international est moindre (3) jusqu'à présent l'impact des attaques est plus local que global**

Technlogies émergentes et cyberrésilience

Quelques chiffres et motivations pour la cyberrésilience

A l'aire

(1) de la révolution du quantum computing : démultiplication énorme des capacités des attaquants, menace sur la cryptographie et avancée extraordinaire dans beaucoup de domaines des sciences et des technologies

(2) de la révolution du génie logiciel par l'IA) : TuringBots, IA capables d'assister les codeurs (et les attaquants !) dans l'écriture de programme et la gestion du développement

(3) du dynamisme renforcé du Dark Web : accès simplifié aux technologies et techniques d'attaques, accès aux vulnérabilités zero day, espace de valorisation des produits des attaques

(4) des attaques recurrents sur les infrastructures critiques : Health Service iralandais en 2021, Colonial Pipeline en 2021, SolarWinds en 2020, Centrifugeuses iraniennes/malware Stuxnet en 2010, Bourse de Nouvelle-Zélande en 2020

Technlogies émergentes et cyberrésilience

Quelques chiffres et motivations pour la cyberrésilience

(5) **de la désinformation de masse, du cyberespionnage et de la guerre des drones** : activistes politiques ou idéologiques, réseaux de cybercriminels, agences de renseignement, groupes terroristes, Etats vayous,
(6) **des zones de libres échanges** : augumentation des cybermenaces liés à la concurrence
(7) **de la diversié et de la complexité des technologies et des systèmes d'information**

sécuriser le cyberespace devient de plus plus un grand challenge pour tous.

Technlogies émergentes et cyberrésilience

A. Cyberrésilience Enjeux et Défis (1)

(0a) **Confiance et sérénité dans le cyberespace :Favoriser le développement des nouvelles transformations sociales et technologiques parmi lesquelles** :

- **les réseaux sociaux**
- **la généralisation du télétravail depuis le Covid19**
- **la dématérialisation des services gouvernementaux** : État civil, Impôts, gestion du personnel, gestion du foncier,...
- **l'automatisation des processus métiers des infrastructures critiques** : eau, énergie, ports, transport,...
- **la digitalisation des métiers et services** : santé, commerce, transport, enseignement, ...
- **les technologies émergentes** : Informatique quantique, RV/RA, Big Data, Cloud, Blockchain, Imprimante 3D, IoT, Drones, Intelligence artificielle, Robotique, 5G/6G. . .

II. Cyberrésilience

II.2 : Cyberrésilience, Enjeux (3) Citoyen

(0b) Les enjeux du citoyen sont à confondre avec les problèmes fondamentaux qui le préoccupe :

- Le caractère fonctionnel, opérationnel et la simplicité d'exploitation des technologies de l'information
- **La Sécurité native dans les systèmes d'information**
- La Confiance dans les technologies de sécurité utilisées
- **La Protection des données personnelles dans le cyberespace**
- La Protection des libertés individuelles dans le cyberespace
- La Protection de la propriété intellectuelle
- **L'éthique et l'équité**

II. Cyberrésilience

II.2 : Cyberrésilience, Enjeux (4) Entreprise (1)

(0c) La majorité du patrimoine de l'entreprise :

- Plans de recherche,
- Résultats de recherche, brevets, Prototypes,
- Politique organisationnelle
- Politique de sécurité
- Plan marketing, Stratégie commerciale,
- Fichiers clients, Contrats (vente, achat, assurance,. . ..)

est susceptible d'être compromis suite à des cyberattaques à cause de la digitalisation quasi – intégrale aujourd'hui.

II. Cyberrésilience

II.2 : Cyberrésilience, Enjeux (5) Entreprise (2)

(0d) Ce qui fait que les enejux et défis classiques de l'entreprise :

- la protection du patrimoine,
- la sauvegarde de l'image,
- la gestion de la concurrence,
- la rentabilité des investissements,
- la garantie de pérennité (de fonctionnement)

sont devenus aussi des enjeux pour la cybersécurité.

Technlogies émergentes et cyberrésilience

A. Cyberrésilience Enjeux et Défis (2)

(1) **Développer des capacités de résilience pour**
(11) faire face aux attaques les plus dévastatrices : le vol de données des entreprises et des Etats, le vol d'identité des travailleurs et des citoyens, les infections ransomwares, les attaques DDOS, les campagnes de désinformation, le cyberespionnage etc.
(12) et verrouiller les premiers vecteurs d'attaques : l'ingenierie social avancée, les moyens d'accès distants, les données d'identification, les vulnérabilités zero day des logiciels métiers et des technologies de sécurité, les erreurs de choix et les défauts de configuration logiciel & matériel ou réseau & Internet, l'usage de la messagerie etc.,
(13) afin de protéger les technologies et acteurs du cyberespace (citoyens, entreprises& organisations nationales et internationales, Etats)

Technlogies émergentes et cyberrésilience

A. Cyberrésilience Enjeux et Défis (3)

(2) **Remedier au faible engagement des pays africains** car selon l'**UIT** (en 2021), "*les niveaux d'engagement de l'Afrique en matière de cybersécurité - ainsi que la capacité de réponse aux menaces - restent faibles par rapport aux autres continents*,
(3) **Remedier à la faible adoption des technologies de cyberrésileince les plus fondementales tels que : (a) Public Key Infrastructure (PKI), (b) Zero Trust Architecture (ZTA), (c) Proactive Domain Name System (PDNS), (d) Phishing-resistant MultiFactor Authentication (MFA) etc.**

A. Cyberrésilience

A. Cyberrésilience Enjeux et Défis (4)

(4) lutter contre la perception qui amoindrit la dangérosité des attaques cibercriminelles, ,
(5) gérer la difficulté de trouver des preuves qui incriminent les criminels surtout s'il s'agit des Etats, ,
(6) combattre la fréquente retention d'informations sur les attaques pour des raisons d'image commerciale ou de marque ce qui rend difficile le travail des CERTs

Technlogies émergentes et cyberrésilience

A. Cyberrésilience, Enjeux et Défis (5)

(7) Protéger les infrastructures et les systèmes vitaux : sociétés de telecoms, armée, smart city, cable sous-marin, cloud national, intranet national, e-services publics, satellites, hopitaux, banques, barrages, aéroports, ports, approvisionnement (eau, electricité, gaz, carburant, alimentation) ;
(8) Se doter de moyens pour la cyberguerre : un commandement de la cyberdéfense pour l'armée, capacité de renseignement et de surveillance automatisés, capacité de pénétration des systèmes hautement sécurisés, moyens de guerre électronique et de guerre économique

Technlogies émergentes et cyberrésilience

A. Cyberrésilience, Enjeux et Défis (6)

(9) Intégrer la cyberdéfense (de concert avec une Politique nationale de digitalisation) comme une composante stratégique dans les entreprises et les 8 ministères suivants : Armées/Renseignement (Haut commandement de la Cyberdefense), Sécurité intérieure (Division Cybercriminalité), Telecoms, Industrie et PME, Finances, Affaires étrangères, Santé, Enseignement supérieur et Recherche
(10) Faire face aux actions subversives des agences publiques ou privées de renseignement, des traffiquants et des groupes terroristes dans le cyberespace africain (Technologies cryptées, Dark web, Désinformation, Cyberrenseignement, Attaques et surveillance par drones, menace sur les OIVs)

Technlogies émergentes et cyberrésilience

A. Cyberrésilience, Enjeux et Défis (7)

- (11) Avoir une maitrise minimale sur la technologie (ordinateur, téléphone, équipements réseaux, protocoles de sécurité) et sur les achitectures fondementales (Cloud national, Intranet national, supercalculateur, laboratoires de fabrication) pour la souveraineté des pays africains :
  Etre capable d'avoir un contrôle (juridique, technique, organisationnel) sur les chaines de valeur pour avoir des équipements sécurisés et
  sans porte dérobée ou éléments étrangers

II. Cyberrésilience

II.3 : Cyberrésilience, Défis/Contrôle technologique (2)

(12-1) **Gendarmerie francaise, 2008** : Il était annoncé en 2008 qu'elle passerait ses 70 000 PC sous Ubuntu avec un contrôle sur les serveurs de mises à jour

(12-2) **Bippeurs du Hezbollah, 2024** : l'explosion des bippeurs du Hezbollah a causé beacoup de dégats humains au Liban et en Syrie

(12-3) **Smartphones Android, 2016** : Kryptowire affirme avoir repéré une porte dérobée dans des smartphones chinois Android low-cost

(12-4) **Espionnage Pegasus 2021** : Pegasus exploitait des failles des téléphones pour faire du espionnage contre des politiques

(12-5) **Vulnérabilité Debian-OpenSSL, 2006** : OpenSSL est packagé par Debian en 2006 avec des erreurs involontaires

(12-6) **ProFTPd, 2010** : un logiciel d'archivage du serveur FTP ProFTPd a été remplacé par une version contenant une porte dérobée.

II. Cyberrésilience

II.3 : Cyberrésilience, Défis (2)

- (3a) assurer la cyberrésilience IoT (IoT domestique, IoT medical, IoT humain, IoT industriel) :
  IoT des smartphones (NFC, Bluetooth, GPS, Wifi, capteur de luminosité et de température, empreinte digitale, altimètre), IoT d'un train (capteurs de données : géolocalisation du train, vitesse du train, niveau d'usure des freins, poids du train, température des essieux), IoT domestique (appareils photo, lumières, thermostats, serrures, caméras de surveillance, consoles de jeux, appareils électroménagers, babyphone)
  La cyberrésilience IoT necessite de controler la conception, la fabrication et la mise sur le marché :
  tolérance aux fautes, absence de porte dérobées, absence d'élements étrangers, sécurité et sureté de fonctionnement (sécurité electronique, sécurité des codes, sécurité des protocoles, cryptographie à bas coût, blockchain, IA, Cloud),

II. Cyberrésilience

II.3 : Cyberrésilience, Défis (2)

Pour la cyberrésilience technologies IoT, plusieurs normes et réglementations sont prises ces dernières années

- En 2018 ; la Chine publie le "China's Internet of Things Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission
- En 2022, le NIST des USA a produit " **Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products**",
- E,n 2022 Le Royaume Uni a adopté la loi "**The Product Security and Telecommunications Infrastructure (PSTI) Act**" pour gérer la cyberrésilience IoT.
- en 2022, l'Union Européenne publie le **Cyber Resilient Act** et l'adopte définitvement en 2024

Cyberrésilience

Cyberrésilience, Enjeux et Défis (8)

- (13b) Gérer la montée en puissance des hackeurs : attaquer est devenu très rentable, **les outils de piratage et la formation des hackeurs sont de plus en plus accessible grâce au Dark Web**,
- (14) Définir et appliquer des politiques adaptées (stratégie et politique nationales de cyberrésilience, législation, réglementation et normalisation, régulation, politiques sectorielles, coopération juridique)

Cyberrésilience

Cyberrésilience, Enjeux et Défis (10)

(15) Menaces sur les systèmes des armées : Aujourd'hui, les armées digitalisent leur métier : **système de combat** (air, sol, mer, cyber), **techniques et outils de cyberguerre** (création d'un commandement de cyberdéfense), **systèmes électroniques, robots, drones, formation virtuelle des combattants et suivi en temps réel des opérations militaires**.
Une attaque sur les systèmes militaires peut conduire de manière directe à des pertes de nombreuses vies humaines, des fuites de données confidentielles (stratégies militaires, nature des équipements et de l'organisation, actions diplomatiques) et un affaiblissement du pays.

Technlogies émergentes et cyberrésilience

Cyberrésilience, Enjeux et Défis (8)

- (16) Mettre en place des institutions d'accompagnement Agences (Cyberrésilience, Cryptologie, Protection des données personnelles), Police/Section cybercriminalité, Armée/commandement de la cyberdéfense, CERTs, SOCs, Centre recherche, Filières de formation),
- (17) Exploiter localement un maillon des chaines de valeur (IoT, cartes à puce, Cryptologie, IA, logiciels de sécurité)
- (18) Trouver des financements conséquents : **le nerf de la guerre** ! !

Recommandations aux états africains (1)

(R2) Stratégie et Politique nationale de cyberrésilience.

1. Décliner une vision opérationalisée dans une politque
2. Posséder des textes législatifs et réglementaires
3. Confier le pilotage de la cyberdéfense nationale à l'armée (commandement de la cyberdéfense) et la cyberrésilience des entreprises et organisations privées à une agence civile
4. Créer un Centre de recherche sur la cyberrésilience et les technologies émergeantes connexes
5. Créer plusieurs formations accadémiques
6. Créer une Agence de protection des Données Personnelles
7. Créer plusieurs PKI sectoriels
8. Créer un CERT (computer emergency response team) / CSIRT national, des SOCs (Security Operation Center) et des CERTs locaux

MERCI DE VOTRE ATTENTION